SECUREAUTH

SecureAuth IdP

Integrated: 2-Factor Authentication, SSO, IdM, Federation, and Mobile

2-Factor Authentication

Multi-factor authentication, either 2- or 3-Factor, is essential in maintaining corporate security. 2FA authenticates users by taking something that they know (username/password) and validating it with something that they have (phone, e-mail, token, device, etc.)

Users submit any enterprise ID into the IdP and gain access into the web, network, cloud, and mobile resources once the SecureAuth authentication conditions are met. This ensures that only valid users can enter applications even if credentials are compromised.

With SecureAuth IdP, companies do not need to restructure their present directory and resource environments because it integrates seamlessly into them. It works with pre-existing data stores so that enterprise information remains in the secured network rather than duplicated elsewhere. 2FA can be applied to existing corporate VPNs or directly into the web, mobile, and SaaS resources.

2FA can be required for any and all devices, including mobile. Admins can easily configure the workflow, authentication, and SSO at any time.

"Device Fingerprinting" is a revolutionary function where devices are logged and linked to users. SecureAuth IdP pulls unique characteristics from each device (desktop or mobile) and maps them to the enterprise directory. This enables low-friction subsequent authentications as users are not required to supply an OTP or token upon device recognition.

Single Sign-on

SecureAuth IdP enables transparent SSO to and between all web, cloud, and mobile applications without additional coding or third-party tools. The integration enables users to use a single credential, regardless of the plethora of enterprise resources.

Internal Web Application SSO allows in-office users to seamlessly access applications (web and SaaS) once logged into the AD domain. By validating the identity through SecureAuth AD SSO, users can enter web and SaaS applications without signing into each one individually. The SSO provides users frictionless access to the cloud resources into which they desire admission.

Cloud Application SSO is achieved through SecureAuth IdP's turnkey portal. Once the IdP consumes and authenticates the IDs, the Security Token Services (STS) translate them into appropriate artifacts, such as SAML, WS-Federation, or OpenID. These federated IDs can then communicate with any cloud application and users gain entrance from the original login.

SecureAuth IdP includes a robust Portal for secure access for all authenticated users to all applications. The portal provides both integrated AD SSO/2FA and SSO for internal and external users.

Mobile Applications Management (MAM) is a distinctive feature of SecureAuth IdP that enables 2FA and SSO to and between native mobile applications. SecureAuth uniquely requires no thick client or special tools for MAM across iOS, Android, and Windows platforms.

SecureAuth IdP enables SSO between the native mobile applications without additional sign-on. Enterprises can even decide to require 2FA for Mobile Applications, which would prompt users to authenticate the application every session, 10 days, 30 days, 90 days, etc.

Identity Management Made Simple

IdM is accomplished in a browser-based GUI admin console that allows preferences to be set through drop-downs and single clicks. SecureAuth IdP requires no hardware, installations, or coding – everything comes built into the system, prepared for out-of-the-box deployment.

Self User Management is also offered. Users can enroll themselves, update profiles, register authentication methods, and reset passwords. These functions can all be accomplished without assistance, which significantly decreases overhead admin help desk costs.

Logging and Auditing tools are other helpful features of SecureAuth IdP. Admins can manage the actions of all users, groups, applications, and devices and make any necessary changes.

With SecureAuth, companies can designate permissions and enforce 2FA and SSO for users, groups, and applications meeting internal and external security standards, including FFIEC, PCI DSS, NCUA HIPAA, and HiTech.

SecureAuth IdP enables organizations to design the security system that they want and the simplicity to enforce this security.

Tel: +1 949-777-6959 www.secureauth.com

SecureAuth IdP provides simple and secure 2-Factor Authentication for all users.

22 Authentication Mechanisms

- SMS, Telephony, E-mail OTP
- Static PIN, KBA/KBQ, Password
- Yubikey (USB), Kerberos (IWA)
- X.509 Native, X.509 Java
- NFC Prox Card, CAC/PIV Card
- Mobile OATH Token
- Browser OATH Token
- Windows Desktop OATH Token
- Third-party OATH Token
- PUSH Notification, Help Desk
- Social IDs, Federated IDs
- Device Fingerprinting, Symantic VIP

Integrated with Existing Data Stores

- AD, v3, LDAPs, SQL
- ODBC, REST APIs
- Google Data Store, Web Services

Flexible and Configurable Authentication

- Based on User, Group
- Application, Device

"Step-up"/Contextual Authentication

- Based on Risk Factors, such as Location or Device Change

Single Sign-on and Identity Management Services for user convenience and simple access control.

Single Sign-on to and between

- Web Apps, Cloud Apps
- Mobile Apps, Network Resources

Internal Web Apps SSO

- Active Directory SSO
- Transparent Navigation
- Desktop Sign-on

Security Token Services (STS)

- Generates Federated Artifacts
- Secure Portal for Point of Access to Cloud Apps

Supported Federated Domains

- SAML, OpenID, WS-Fed/Trust
- ADFS, OAuth, Liberty Alliance

Supports Application Protocols

- RADIUS, LTPA, SAML
- J2EE, F5 Session Tokens, and others

Identity Management Tools

Logging and Auditing

- Users, Groups
- Devices, Applications
- Authentication Events

User Self-services

- Profile Management
- 2-Factor Enrollment
- Password Reset

Browser-based GUI Console

1-Touch Revocation

Mobile 2-Factor Authentication and SSO Support

- iOS, Android
- Windows, Blackberry

SECUREAUTH

2-Factor Access Control for the Mobile Enterprise